Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently amended) An apparatus for transmitting a file through a network, the apparatus comprising:

a file-splitting processor for splitting a file into a plurality of message segments and assigning one of a plurality of final destination addresses to each segment, the plurality of final destination addresses being assigned to a receiving host; and

a message segment transmitter for transmitting the plurality of message segments to the receiving host using the plurality of final destination addresses.

2. (Previously presented) The apparatus of claim 1 wherein the file-splitting processor further comprises a file converter for converting the file into N message segments such that the file is reassemblable from a subset of any K of the message segments at the receiving host, N and K being positive integers and $N > K > 1$.

3. (Currently amended) The apparatus of claim 1 wherein the file-splitting processor is configured for assigning one of a plurality of initial source addresses to each of the plurality of message segments, thereby impeding attempts to ascertain the source of the file.

4. (Previously presented) The apparatus of claim 1, further comprising a message segment monitor for detecting non-receipt of a subset of the plurality of message segments.

5. (Previously presented) The apparatus of claim 1, further comprising an address allocator for assigning a subset of the plurality of destination addresses to the receiving host.

6. (Currently amended) An apparatus for transmitting a file through a network, the apparatus comprising:

a file-splitting processor for splitting the file into a plurality of message segments and assigning one of a plurality of initial source addresses to each message segment of the plurality of message segments, thereby disguising the origin of the file; and

a message segment transmitter for transmitting the plurality of message segments to a receiving host.

7. (Currently amended) The apparatus of claim 6 wherein the file-splitting processor is configured for assigning one of a plurality of final destination addresses assigned to the receiving host to each message segment of the plurality of message segments.

8. (Currently amended) A method for securely transmitting a file through a network, the method comprising:

(a) at a source host, splitting the file into a plurality of message segments;

(b) addressing, at the source host, each message segment of the plurality of message segments using one of a plurality of final destination addresses assigned to a receiving host; and

(c) transmitting the plurality of message segments to the receiving host with the plurality of final destination addresses.

9. (Previously presented) The method of claim 8 wherein the plurality of message segments are addressed in one-to-one correspondence to at least a subset of the plurality of destination addresses.

10. (Previously presented) The method claim 8 wherein splitting the file into a plurality of message segments comprises converting the file into N message segments such that the file is reassemblable from a subset of any K of the message segments, N and K being positive integers and $N > K > 1$.

11. (Currently amended) The method of claim 10, further comprising assigning N final destination addresses to the receiving host, wherein the N message segments are addressed using

one of the N final destination addresses assigned to the receiving host.

12. (Currently amended) The method of claim 11, further comprising causing the receiving host to cease receiving messages on at least one of the N final destination addresses in response to an attack on the at least one of the final destination addresses.

13. (Currently amended) The method of claim 12 wherein the receiving host ceases to receive messages via no more than (N-K) final destination addresses, thereby facilitating reassembly of the file by the host.

14. (Currently amended) The method of claim 11, further comprising:

(e) reassembling the N message segments into a reassembled file at the receiving host;

(f) splitting the reassembled file into a second set of N message segments at the receiving host; and

(g) transmitting the second set of N message segments from the receiving host using the N final destination addresses.

15. (Previously presented) The method of claim 8, further comprising:

(d) retransmitting the plurality of message segments from the receiving host.

16. (Previously presented) The method of claim 15 wherein retransmitting the plurality of message segments from the receiving host comprises retransmitting the plurality of message segments to at least two of a plurality of intermediate hosts, thereby relaying the plurality of message segments along more than one path through the network.

17. (Previously presented) The method of claim 8, further comprising:

(d) selecting a virtual network comprising a plurality of hosts, the plurality of hosts including the receiving host;

(e) assigning each host of the plurality of hosts to a domain of a plurality of domains;

(f) designating sets of the host pairs, each host pair comprising two hosts assigned to the same domain or a neighboring domain; and

(g) constraining travel of each message segment of the plurality of message segments to the receiving host via relays between host pairs.

18. (Currently amended) The method of claim 8, further comprising:

(d) assigning a source address selected from a plurality of initial source addresses to each message segment of the plurality of message segments, thereby impeding attempts to ascertain the source of the file.

19. (Previously presented) The method of claim 8, further comprising:

(d) receiving, at the receiving host, at least a portion of the plurality of message segments;

(e) reassembling the file from the received message segments at the receiving host;

(f) splitting the reassembled file into a second plurality of message segments at the receiving host; and

(g) transmitting the second plurality of message segments from the receiving host.

20. (Previously presented) The method of claim 8 wherein step (c) comprises transmitting the plurality of message segments to at least one of an intermediate host and a destination host.

21. (Previously presented) The method of claim 8 wherein step (c) comprises transmitting from at least one of a source host and an intermediate host.

22. (Currently amended) The method of claim 8, further comprising:

~~(d)~~ monitoring non-receipt by the receiving host of at least one of the plurality of message segments.

23. (Currently amended) The method of claim 8, further comprising:

(d) allocating M final destination addresses for assignment to the receiving host;

(e) assigning N final destination addresses of the M allocated final destination addresses, where N is less than or equal to M; and

(e) periodically reassigning to the receiving host at least a portion of the N final destination addresses.

24. (Currently amended) The method of claim 10, further comprising:

(d) periodically reassigning at least a subset of the plurality of final destination addresses assigned to the receiving host while leaving at least K of the final destination addresses unchanged thereby permitting continuous receipt of messages by the receiving host, and

(e) notifying at least a portion of the network of the reassigned final destination addresses.

25. (Previously presented) The method of claim 8, further comprising:

(d) adding status information associated with a sending host to the message segment; and

(e) upon receipt by the receiving host, interpreting the status information to detect tampering with message segment transmission.

26. (Previously presented) The method of claim 8, further comprising:

(d) encoding the file to produce an encoded bit file having encoded bits, and

(e) scrambling the encoded bits, such that the encoded bit file is split into a plurality of message segments.

27. (Currently amended) A method of securely transmitting a file through a network, the method comprising:

(a) splitting the file into a plurality of message segments at a source host;

(b) at the source host, assigning one initial source address of a plurality of initial source addresses to each message segment of the plurality of message segments, thereby disguising the origin of the file; and

(c) transmitting the plurality of message segments.

28. (Currently amended) The method of claim 27, further comprising:

(d) assigning one final destination address of a plurality of final destination addresses assigned to a receiving host to each message segment of the plurality of message segments.

29. (Currently amended) A method for securely transmitting a file through a network, the method comprising:

(a) splitting the file into a plurality of message segments, each message segment comprising a final destination specifier, encrypted protocol information, and encrypted message data;

(b) receiving a message segment at a receiving host;

(c) decrypting the message data to determine a destination host;

(d) encrypting the message data in accordance with an encryption protocol accessible to the destination host;

(e) transmitting the encrypted message segment to the final destination host; and

(f) repeating steps (a)-(e) for other message segments, thereby facilitating recovery of the message by the destination host.

30. (Previously presented) The method of claim 29 wherein the message segment has a length, and further comprising altering the length.

31. (Previously presented) The method of claim 29 wherein the receiving host and the destination host negotiate to determine the encryption protocol.

32. (Previously presented) The method of claim 29, further comprising causing the receiving host to adding status information concerning the receiving host to the message segment, and, at

the receiving host, interpreting the status information to detect tampering with message segment transmission.

33. (Previously presented) A method for defining and operating a network topology to camouflage network traffic patterns and volume, the network comprising a plurality of hosts, the method comprising:

(a) assigning each host of a plurality of hosts to a first domain of a plurality of domains; and

(b) restricting network traffic to message transmissions among hosts within the same domain or neighboring domains, thereby defining multiple redundant relay paths among hosts, thereby camouflaging message sources and destinations.

34. (Previously presented) The method of claim 33, further comprising:

(c) reassigning at least one host of the plurality of the hosts to a second domain of the plurality of domains, thereby changing network traffic patterns.

35. (Currently amended) The method of claim 33, further comprising:

(d) assigning one of a plurality of final addresses selected from a pool of final addresses assigned to ~~with~~ each one of the plurality of hosts;

(e) reassigning at least one of the plurality of assigned final addresses from the pool of final addresses; and

(f) notifying the plurality of hosts of the reassigned addresses.

36. (Previously presented) The method of claim 35 wherein a portion of the plurality of addresses is reassigned at any one time to permit the use of addresses not having been reassigned for notifying the plurality of hosts of the reassigned addresses.